L'entreprise et la sécurité nationale

Bertrand PAUVERT
Maître de conférences HDR à l'Université de Haute-Alsace

Entreprise et sécurité nationale ; lier les deux termes peut sembler paradoxal tant il est vrai que les réalités qu'ils recouvrent paraissent relativement étrangères l'une à l'autre. En effet et au-delà de sa définition précise, la sécurité nationale évoque naturellement l'idée de survie de la nation et donc les compétences régaliennes, quant l'entreprise, pour sa part, illustre tout aussi spontanément la notion d'intérêts strictement privés et la recherche de profits. Il convient pourtant de ne pas en rester à cette courte vue, mais bien se rappeler que l'entreprise, loin de ne satisfaire que les seuls intérêts légitimes de ses propriétaires, possède bien évidemment une utilité commune, une fonction sociale. Deux éléments justifient que l'entreprise mérite de se voir envisagée à l'aune de son rapport avec la sécurité nationale.

D'une part, il a de longue date été constaté que les questions de défense et de sécurité ne pouvaient faire l'économie d'une réflexion sur leurs dimensions économiques, soit qu'il s'agisse simplement du coût d'un conflit, soit encore que l'on envisage la seule question de la satisfaction par l'économie des besoins militaires liés à ce conflit. D'autre part, le concept de sécurité nationale, tel qu'il a été théorisé par les Livres Blancs de 2008 et 2013, fait la part belle à une vision élargie des enjeux de sécurité et de défense[1], la loi consacrant cette approche en disposant que « *la stratégie de sécurité nationale a pour objet d'identifier l'ensemble des menaces et des risques susceptibles d'affecter la vie de la Nation, notamment en ce qui concerne la protection de la population, l'intégrité du territoire et la permanence des institutions de la République, et de déterminer les réponses que les pouvoirs publics doivent y apporter* »[2]. Cette vision élargie de la Défense consacrée par la notion de sécurité nationale justifie qu'une plus grande attention soit désormais apportée aux questions économiques ; c'est ainsi que si le Livre Blanc de 1994 n'évoquait que très rapidement la seule « défense économique »[3] et que l'*opus* de 2008 n'en soufflait mot, le Livre Blanc de

[1] On se permettra de renvoyer à notre étude, « 1972 - 2013, Quarante ans de Livres Blanc, permanences et évolutions de l'impératif de Défense en France », in *Le droit de la sécurité et de la défense en 2013*, Ch. Vallar et X. Latour dir., PU Aix-Marseille, 2014, pp. 51-62.
[2] Art. L. 1111-1 du code de la défense.
[3] *Livre blanc sur la Défense*, La Doc. fr., 1994, p. 155. D'ailleurs, les termes alors employés pour aborder les questions économiques attestent d'une proximité très grande avec ceux figurant dans la défunte ordonnance du 7 janvier 1959 portant organisation générale de la défense.

2013 y consacra au contraire trois pages pleines, attestant de la dimension aujourd'hui cardinale de la dimension économique de la sécurité nationale[4]. A dire vrai cela ne saurait surprendre, chacun pouvant se souvenir de la formule prononcée en 1953 par celui qui allait devenir le secrétaire d'Etat à la Défense du président Eisenhower, Charles Wilson et selon laquelle « *tout ce qui est bon pour General Motors est bon pour l'Amérique* »[5] ; à la même époque, la France, par l'ordonnance du 7 janvier 1959 portant organisation générale de la défense, consacrait d'ailleurs explicitement la notion de « défense économique ».

Pour autant, cette « défense économique » est restée -et reste encore- le parent pauvre de la réflexion sur la Défense et « *la Défense économique n'a pas su, malgré l'ardente impulsion de Monsieur Debré, profiter de la motivation qu'elle avait suscitée ni, sur sa lancée, confirmer ses réalisations initiales. Le vide ainsi créé par l'absence prolongée d'impulsion ministérielle a privilégié naturellement les préoccupations d'ordre public et de protection des populations, déséquilibrant l'architecture logique de la Défense non militaire, telle qu'elle avait été conçue par l'ordonnance de 1959* »[6]. Effectué il y a plus de 20 ans, ce constat reste exact et la défense économique reste très loin de ce qu'elle pourrait être, ne possédant qu'une dimension limitée, simple « *héritière de l'organisation mise en place pendant les périodes de guerre* »[7]. Derrière la façade d'un discours officiel la valorisant, la défense économique n'a pas pu conquérir une autonomie réelle par rapport à une défense militaire au service de laquelle elle demeure intimement liée ; les questions de Défense et de Sécurité ont le plus souvent été appréhendées sous les angles kaki voire bleu marine, sans que l'on envisage sérieusement la place du costume cravate ou du bleu de travail en leur sein.

Or, l'importance des entreprises sous l'angle d'une perception globale de la sécurité nationale est pourtant vitale, quand leur participation active aux missions de sécurité est encore trop souvent négligée. Si la stratégie de sécurité nationale initiée par l'Etat a effectivement pour objet « *d'identifier l'ensemble des menaces et des risques susceptibles d'affecter la vie de la Nation (…) et de déterminer les réponses que les pouvoirs publics doivent y apporter* », alors les enjeux liés à la stabilité de l'économie et au dynamisme des entreprises s'inscrivent incontestablement au cœur de cette stratégie. L'Etat ne peut rester

[4] *Livre Blanc - Défense et sécurité nationale*, Direction de l'information légale et administrative, Paris, 2013, pp. 105-107.

[5] Charles Wilson, ancien président directeur-général de General Motors, prononce ces mots devant le Sénat, lorsque celui-ci l'interrogeait, avant sa nomination, à propos d'éventuels conflits d'intérêts entre ses fonctions au sein du groupe automobile et son futur poste de Secrétaire à la Défense.

[6] Jean Bontoux, « Un outil de prévention et de gestion des crises : la Défense économique », *Les Notes Bleues de Bercy*, 1993, n° 8, 20 p.

[7] Didier Danet, « La Défense économique, une structure en quête d'identité ? », in *Industrie, Technologie et Défense*, Bertrand Warusfel dir., Centre Droit et Défense, La Doc. fr., 1993.

indifférent aux entreprises composant le tissu économique du pays et à la source de la création de richesses, d'embauche et générant, au-delà, des moyens d'action pour la puissance publique. La France dispose ainsi d'un maillage entrepreneurial de plus de trois millions d'entreprises, quand les seules entreprises marchandes (de production de bien et de service) représentaient à elles seules 55% du produit intérieur brut, pour un chiffre d'affaire atteignant près de quatre milliards d'euros[8]. Ces quelques chiffres démontrent l'importance de l'économie et des entreprises pour la France et justifient que l'Etat ne reste pas indifférent à leur activité. Si l'Etat n'a certes pas vocation à administrer l'économie de manière directe, il recherchera des moyens d'assurer la pérennité des flux économiques essentiels à la vie de la Nation ; dès lors la question des rapports entre entreprise et sécurité nationale vise à apprécier la manière dont gouvernants et acteurs économiques interagissent de manière à sauvegarder les intérêts économiques de la Nation.

Conscient des risques et des faiblesses qui pèsent sur son économie et par extension sur la Nation, la puissance publique prend un certain nombre d'actes et d'initiatives « *d'une part pour protéger et défendre l'économie et les entreprises des atteintes de toute nature et, d'autre part, pour subvenir aux besoins de la défense nationale* »[9]. L'Etat, s'adaptant aux circonstances, agit à titre préventif et curatif, en soutien de l'activité économique des entreprises ; prévention et réparation visant à donner aux acteurs économiques les moyens de faire face à des crises de toutes sortes affectant l'économie du pays. Cette mission est mise à la charge du ministre chargé de l'économie, « *responsable de la préparation et de l'exécution de la politique de sécurité économique. Il prend les mesures de sa compétence garantissant la continuité de l'activité économique en cas de crise majeure et assure la protection des intérêts économiques de la Nation* »[10]. L'idée d'une nécessaire intervention de l'Etat dans le monde de l'entreprise, au titre de la sécurité économique, doit beaucoup à la rénovation de la réflexion ayant accompagné l'essor de la notion d'intelligence économique[11]. Dans un contexte de globalisation des échanges et des flux économiques, d'interconnexion des économies et d'ouverture à l'information, il est acquis que les entreprises nationales soutenues par leur Etat se livrent une « guerre économique » sur le marché international[12]. Dans ce cadre, la concurrence exacerbée entre entreprises ne concerne plus uniquement les biens et les

[8] INSEE, *Les entreprises en France*, éd. 2013, www.insee.fr/fr/ffc/docs_ffc/ENTFRA13.pdf, p. 126
[9] Circulaire du 14 fév. 2002 relative à la défense économique (JO du 23, p. 5164).
[10] Art. L. 1142-3 du code de la défense. Il est par ailleurs chargé d'orienter l'action des ministres responsables de la production, de l'approvisionnement et de l'utilisation des ressources nécessaires à la défense et à la sécurité nationale.
[11] V. not. le rapport précurseur du Commissariat général au Plan, réalisé par Henri Martre, *Intelligence économique et stratégie des entreprises*, La Doc. fr., 1994.
[12] V. not. Christian Harbulot, *La machine de guerre économique*, Economica, Paris, 1992.

services, mais s'est encore ouverte aux éléments immatériels, à la propriété intellectuelle et industrielle, aux images et aux logiciels : c'est l'avènement d'une concurrence d'un nouveau type qui s'exerce bien en amont de la production et porte aussi sur des questions d'innovation et de conception des produits.

Au-delà du seul soutien à une industrie de défense autonome rendant la nation indépendante des partenaires de la France, l'Etat intervient au cœur de cette guerre économique nouvelle et dans ce cadre mouvant. Pour les pouvoirs publics, il est un impératif absolu pour la sécurité nationale de diminuer la vulnérabilité des entreprises ; au-delà, accompagner la réactivité de ces entreprises, constitue un enjeu tout aussi fondamental.

1. Diminuer la vulnérabilité des entreprises, un enjeu de sécurité nationale

Envisagée sous l'angle de la sécurité nationale, la vulnérabilité des entreprises peut s'entendre de deux manières distinctes ; celle des personnes travaillant en leur sein ou celle des sites industriels en eux-mêmes. Au regard de l'activité des entreprises, c'est un enjeu de sécurité nationale de veiller à ce que les personnels qu'elles emploient ne soient pas source de vulnérabilité ; de manière semblable, certains sites représentent en eux-mêmes des enjeux pour la sécurité nationale, au regard des conséquences que pourraient avoir leur destruction. Diminuer la vulnérabilité des entreprises suppose d'agir vis-à-vis des personnes et des sites.

1.1. La vulnérabilité des personnes

Au regard de la sécurité nationale, une attention particulière mérite d'être portée sur le personnel de certaines entreprises ; présentant un enjeu de sécurité il est alors important de se prémunir à l'encontre de toute vulnérabilité que ces employés pourraient occasionner. Si de simples enquêtes administratives permettent de vérifier qu'une personne est apte à exercer certaines fonctions, il sera parfois nécessaire de se livrer à une recherche plus approfondi, lorsqu'un agent d'une entreprise doit faire l'objet d'une habilitation secret-défense.

Si la catégorie des « enquêtes administratives » recouvre une multitude de procédures distinctes s'appliquant à nombre de situations hétérogènes, le Code de la sécurité intérieure prévoit que de telles enquêtes soient réalisées dans le but de vérifier la compatibilité du comportement de certaines personnes avec les fonctions et missions qu'elles seraient susceptibles d'exercer ; cela dans le secteur public bien évidemment, mais également au sein d'entreprises privées. D'abord, ces enquêtes s'appliquent aux « *décisions administratives de recrutement, d'affectation, d'autorisation, d'agrément ou d'habilitation (…) concernant les emplois publics participant à l'exercice des missions de souveraineté de l'Etat, soit les*

emplois publics ou privés relevant du domaine de la sécurité ou de la défense »[13] ; en revanche, il est moins connu qu'elles visent encore « *les emplois privés ou activités privées réglementées* », ainsi que « *l'accès à des zones protégées en raison de l'activité qui s'y exerce, l'utilisation de matériels ou produits présentant un caractère dangereux* »[14]. Ces enquêtes sont destinées à vérifier que le comportement des personnes visées ne soit pas incompatible avec l'exercice des fonctions ou des missions envisagées ».

Les opérations d'investigation menées cherchent à déterminer s'il existe des éléments remettant en cause la compatibilité du postulant avec les fonctions ou qualités auxquelles il prétend. Il s'agit bel et bien d'une restriction à la liberté de travailler justifiée par l'exigence du maintien de l'ordre public et le droit à la sécurité ; ce sont les articles R. 114-2 à R. 114-5 du code de la sécurité intérieure qui fixent la liste des décisions pouvant donner lieu à de telles enquêtes administratives préalables. En particulier, outre l'ensemble des personnes travaillant dans le secteur de la sécurité privée, le code mentionne également le personnel des entreprises accédant à des zones considérées comme sensibles au regard de la sécurité intérieure ; par voie de conséquence, toute entreprise souhaitant que son personnel puisse accéder à ces zones doit soumettre celui-ci à enquête administrative[15]. Une telle enquête peut encore être menée à propos des personnes amenées à travailler dans le domaine de la création ou la commercialisation des armes et munitions[16]. Il n'existe pas d'autorité compétente unique en matière d'enquête administrative, mais plusieurs[17], sachant que l'enquête prendra le plus souvent la forme d'une consultation des différents systèmes de traitements de données à caractère personnel ; consultation effectuée par des agents de la police nationale et de la gendarmerie nationale[18], qui prendront connaissance des dispositions figurant dans le traitement des antécédents judiciaires[19]. En particulier a été créé à cet effet un fichier particulier : le traitement des « Enquêtes administratives liées à la sécurité publique »[20].

Le souci de protéger les intérêts de la France est au cœur de la notion de « Secret de la défense nationale ». Celui-ci vise à assurer la sauvegarde des intérêts fondamentaux de la

[13] Art. L. 114-1 CSI. Cela vise donc l'ensemble des professions liées à la sécurité privée.
[14] *Ibid*.
[15] Art. R. 114-4 CSI. Cela correspond notamment aux zones placées sous le contrôle de l'autorité militaire ou mentionnées par le code de la défense (art. L. 1332-1 et 2), le code pénal (art. 413-7), celles non librement accessibles des aérodromes (art. L. 6332-1 du code des transports) ou enfin dans lesquelles sont préparés et stockés le fret aérien ainsi que les biens et produits destinés à être utilisés à bord des aéronefs (art. L. 6342-1 et L. 6343-1 du code des transports).
[16] Art. R. 114-5 CSI.
[17] A titre d'exemple, c'est le Conseil National des Activités Privées de Sécurité qui diligentera les enquêtes lors des demandes d'autorisations des agents privés de sécurité.
[18] Art. L. 234- 2 CSI.
[19] Art. L. 234-1 CSI ; ce traitement est le résultat de la fusion du STIC et du JUDEX.
[20] D. 2009-1250 du 16 oct. 2009 (JO du 18, p. 17.245) le décret est codifié aux art. R. 236-1 à 10 CSI.

Nation dans les domaines de la défense, de la sécurité intérieure et de la protection des activités financières, économiques ou industrielles, de la protection du patrimoine scientifique et culturel de la France. L'idée est donc de limiter l'accès à certaines informations puisque celles-ci « *présentent, en cas de divulgation, un risque tel d'atteinte à la défense et à la sécurité nationale que seules certaines personnes sont autorisées à y accéder* »[21]. Si les gouvernants considèrent qu'une information présente un tel risque, alors ils procèderont à sa classification[22] afin de la faire bénéficier d'une stricte protection et encadrer les personnes susceptibles d'y avoir accès. La classification a pour effet de restreindre l'accès à l'information, elle répond à un besoin de protection qui peut, selon le cas, viser des documents, support, recherches... Simplement, cette nécessité, loin de ne concerner que l'Etat, vise encore des opérateurs économiques, car comme le but est d'éviter que ces informations soient utilisées contre le pays, cela vise donc, outre la question militaire au sens strict, les informations économiques stratégiques[23]. En particulier, les entreprises traitant avec le ministère de la défense sous soumises à différentes procédures[24] dont le respect est assuré par la direction de la protection et de la sécurité de la défense (DPSD) ; contractant avec la Défense, une entreprise (et certains de ses personnels) est en situation d'avoir accès à des informations classifiées, ce qui suppose que soit préalablement vérifiée son aptitude à en connaître[25]. Ces obligations concernent les entreprises les plus connues, mais aussi quantités d'autres structures, laboratoires de recherches ou sous-traitants qui n'auraient pas d'activité « militaire » en tant que telle. Toutes les personnes qui traitent ou doivent avoir connaissance d'information classifiées doivent être habilitées[26], tant il est vrai que l'accès à une telle information par une personne non habilitée fait l'objet d'une incrimination pénale[27].

L'employeur doit établir un « répertoire des personnes habilitées »[28] et déposer une demande d'habilitation pour tout employé dont les fonctions sont susceptibles d'impliquer

[21] Instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale (JO du 2 déc. 2011, p. 20.265)

[22] La classification recouvre une multitude d'information, qui vont de simples notes diplomatiques, au secret de la fabrication nucléaire militaire ; elle se traduit par trois niveaux distincts : le « Très Secret-Défense » (TSD, niveau le plus sensible), « Secret-Défense » (SD, niveau intermédiaire) et le « Confidentiel-Défense » (CD).

[23] On pense notamment aux travaux de recherche ayant indirectement trait à la défense nationale, des négociations commerciales, des procédés de fabrication, du transfert de technologie…

[24] Procédures de protection des données, d'habilitation de certains salariés, de protection des locaux…

[25] L'aptitude désigne la « *capacité d'une entreprise à traiter ou à détenir des informations ou des supports classifiés. Cette capacité, évaluée par un service enquêteur, est fondée sur le contrôle de l'ensemble des mesures de sécurité physique mises en œuvre par le titulaire du contrat pour un ou plusieurs établissements et incluant, si nécessaire, la sécurité des systèmes d'information* », Instruction générale n° 1300 préc., *Glossaire*.

[26] En effet, *« nul n'est qualifié pour connaître des informations et supports classifiés s'il n'a fait au préalable l'objet d'une décision d'habilitation et s'il n'a besoin (...), de les connaître pour l'exercice de sa fonction ou l'accomplissement de sa mission* », art. R. 2311-7 du code de la défense.

[27] Art. 413-10 du code pénal.

[28] Art. 20 de l'Instruction générale n° 1300 préc.

l'accès ou la détention d'informations ou de supports classifiés. Les personnes concernées sont alors l'objet d'une procédure d'enquête personnalisée par les services de sécurité. Le dossier d'habilitation est adressé par l'employeur à l'autorité d'habilitation et l'enquête de sécurité visera à déceler d'éventuels risques chez le candidat[29]. Il s'agit de déterminer si l'intéressé, par son comportement ou par son environnement proche, présente une vulnérabilité, soit parce qu'il constitue lui-même une menace pour le secret, soit parce qu'il se trouve exposé à un risque de chantage ou de pressions pouvant mettre en péril les intérêts de l'Etat[30]. Après instruction du dossier et au regard de l'avis formulé, l'employé pourra se voir habilité[31]. Les obligations pesant sur l'employé ne s'arrêtent d'ailleurs pas au moment de son habilitation mais se poursuivent tout au long de son emploi[32] et même au-delà[33].

Si des personnes employées par les entreprises peuvent être sources de vulnérabilité pour la sécurité nationale et justifient ces enquêtes préalables à leur emploi, il en est de même de certains sites industriels. Il est alors impératif pour la sécurité nationale de restreindre la vulnérabilité de ces sites.

1.2. La vulnérabilité des sites

Différents dispositifs visent à diminuer la vulnérabilité des sites. Tout d'abord et au regard de l'importance des activités qui y sont menées, certains espaces d'entreprises peuvent faire l'objet de dispositifs de protection. Au-delà, certaines entreprises font l'objet d'une réglementation spécifique, celles dont « *la poursuite et le maintien de l'activité en toutes circonstances revêt pour la société dans son ensemble une importance vitale* »[34].

---

[29] Pour le niveau Très Secret Défense, c'est le SGDSN directement qui mène l'enquête, pour les niveaux Secret Défense et Confidentiel Défense, l'enquête de sécurité vise est diligentée selon le cas par le service enquêteur du ministère de l'intérieur (personnels civils ou organismes travaillant dans le domaine civil) ou par celui du ministère de la défense personnels civils ou militaires du ministère de la défense, de la gendarmerie, employés des organismes ou entreprises travaillant au profit du ministère de la défense).

[30] Art. 24 de l'Instruction générale n° 1300 préc. Par ex. : chantage ou pressions exercés par un service étranger de renseignement, un groupe terroriste, une organisation ou une personne se livrant à des activités subversives.

[31] L'habilitation est prononcée selon le cas par le Premier ministre (habilitation TSD) ou pour les autres habilitations par les ministres compétents (il s'agit alors le plus souvent d'une signature du Haut fonctionnaire défense et sécurité du ministère) ou par délégation les préfets ; il est à noter que le refus d'habilitation de la part de l'autorité compétente n'a pas à être motivée : CE, 13 juin 1997, *Min. de la défense*, req. n° 157.252.

[32] L'employé habilité reste tenu à différentes obligations ; en particulier, il est tenu d'informer au plus vite, pendant toute la durée de son habilitation, l'officier de sécurité dont il relève de tout changement affectant sa vie personnelle (mariage, divorce, PACS, établissement ou rupture d'une vie commune...), professionnelle ou son lieu de résidence. Il doit de même informer de toute relation suivie et fréquente dépassant le strict cadre professionnel avec un ou plusieurs ressortissants étrangers. Ces évolutions peuvent justifier un réexamen du dossier d'habilitation et, le cas échéant, le retrait de l'habilitation.

[33] L'employé habilité signe un engagement précisant que les obligations visant à la protection des informations classifiées auxquelles il a pu avoir accès perdurent au-delà du terme mis à ses fonctions ou à son habilitation.

[34] Jérémie Vallotton, « Les entreprises et la sécurité civile », in *Etat des lieux de la sécurité civile en France*, S. Gaultier-Gaillard dir., PU Sorbonne, à par. 2015.

Comme les personnes, les lieux doivent être protégés et c'est ainsi que tous les lieux qui contiennent des données sensibles doivent être protégés. La réglementation distingue à cet effet les zones protégées[35] et les zones réservées[36], peu important en l'espèce que ces espaces relèvent d'une personne publique ou privée. La délimitation de ces zones a pour but d'assurer aux lieux intéressant la défense nationale, qu'il s'agisse de services, d'établissements ou d'entreprises, publiques ou privées, une protection juridique contre les intrusions ; cela permettra donc de protéger les informations et supports qui s'y trouvent ainsi que les systèmes d'information classifiés au niveau Secret Défense. Cette protection des espaces est complémentaire des dispositions concernant les personnes précédemment évoquées et ces zones sont obligatoirement créées dans l'ensemble des services et organismes qui, de manière habituelle, élaborent, traitent, reçoivent ou détiennent des informations ou supports classifiés au niveau Secret Défense. Ces zones sont créées par arrêté des ministres intéressés et font l'objet d'une interdiction d'accès sans autorisation ; interdiction sanctionnée pénalement en cas d'infraction[37]. On rappellera encore qu'au titre de la vulnérabilité des sites ce sont également les systèmes d'information des entreprises intéressant la sécurité nationale qui doivent obtenir une homologation de sécurité ; ce dispositif vise à prévenir des cyberattaques et l'agrément est alors donné par l'Agence Nationale de la Sécurité des Systèmes d'Information.[38]

C'est en 1958 que furent pour la première fois évoquées les installations d'importance vitale[39] et le code de la Défense vise désormais les « *installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation* »[40]. Au lendemain des

[35] La zone protégée consiste en un local ou terrain clos délimité, où la libre circulation est interdite et l'accès soumis à autorisation afin de protéger les installations, les matériels, le secret des recherches, des études ou des fabrications ou les informations ou supports classifiés qui s'y trouvent. Les limites en sont visibles et ne peuvent être franchies par inadvertance. Art. 73 de l'Instruction générale n° 1300 préc.

[36] La zone réservée se trouve toujours dans une zone protégée. Il s'agit d'un local ou emplacement faisant l'objet de mesures de protection matérielle particulières et dont l'accès est réglementé et subordonné à des conditions spéciales. En général, il s'agit du cœur de la zone protégée, là où se trouvent les données sensibles. C'est dans cette zone réservée que se trouve le bureau de protection du secret, lieu obligatoire pour procéder à l'élaboration, au marquage, au stockage, à l'acheminement, à l'enregistrement, au suivi et à la destruction des informations ou supports classifiés Secret Défense. Art. 74 de l'Instruction générale n° 1300 préc.

[37] Art. 413-7 du code pénal.

[38] Art. R. 2311-6-1 du code de la défense.

[39] Ord. n° 58-1371 du 29 déc. 1958 tendant à renforcer la protection des installations d'importance vitale (JO du 31, p. 12.064). Ces entreprises étaient désignées par l'article premier, comme celles : « *exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation* ». L'article ajoutait que ces entreprises étaient « *tenues de coopérer à leurs frais dans les conditions définies au présent chapitre, à la protection desdits établissements, installations et ouvrages contre toute tentative de sabotage* ».

[40] Art. L. 1332-1 du code de la défense.

événements de septembre 2001, la prévention des risques terroristes étaient au cœur des préoccupations des pouvoirs publics lors de la rénovation de cette législation et un secteur d'activité est entendu comme d'importance vitale (SAIV) lorsqu'il est constitué d'activités qui « *1° Ont trait à la production et la distribution de biens ou de services indispensables : a) A la satisfaction des besoins essentiels pour la vie des populations ; b) Ou à l'exercice de l'autorité de l'Etat ; c) Ou au fonctionnement de l'économie ; d) Ou au maintien du potentiel de défense ; e) Ou à la sécurité de la Nation, dès lors que ces activités sont difficilement substituables ou remplaçables ; 2° Ou peuvent présenter un danger grave pour la population* »[41]. C'est le Premier ministre qui détermine les SAIV et adopte, pour chacun d'entre eux, des Directives Nationale de Sécurité[42]. Certaines entreprises peuvent alors être désignées par l'autorité administrative comme des « opérateurs d'importance vitale »[43], dès lors qu'elles gèrent des établissements, ouvrages ou des installations « *dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement : a) D'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ; b) Ou de mettre gravement en cause la santé ou la vie de la population* »[44].

Ces ouvrages sont par la suite désignés par le Code de la défense sous le terme de Points d'Importance Vitale (PIV)[45] ; désignation qui emporte l'obligation pour l'opérateur de se soumettre, à ses frais, à un ensemble de règles particulièrement lourdes. L'entreprise privée exploitant un établissement désigné comme PIV devra d'abord charger l'un de ses employés, d'exercer les fonctions de délégué pour la défense et la sécurité[46] ; cet employé est un véritable « officier de sécurité » de l'entreprise. Nommé par l'employeur, il est le correspondant du Haut fonctionnaire défense et sécurité ainsi que des services enquêteurs. Il a pour mission, de fixer les règles et consignes de sécurité à mettre en œuvre concernant les

[41] Art. R. 1332-2 du code de la défense.
[42] Art. R. 1332-16 à 1332-18 du code de la défense. Celles-ci fixent étroitement le cadre d'action des entreprises auxquelles elles s'appliquent, définissant notamment les « *mesures planifiées et graduées de vigilance, de prévention, de protection et de réaction contre toute menace, notamment à caractère terroriste* », art. R. 1332-17 du code de la défense. Parmi les secteurs en cause, outre le nucléaire ainsi que les activités civiles, militaires et judiciaires de l'Etat, on y trouve l'alimentation, la finance, la gestion de l'eau : arrêté du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs (JO du 4, p. 8502).
[43] Art. R. 1332-3 du code de la défense.
[44] Art. R. 1332-1 du code de la défense.
[45] Art. R. 1332-4 du code de la défense.
[46] Préalablement à sa prise de fonction, cet employé devra recevoir une habilitation « confidentiel défense », art. D. 1332-5-1 et R. 2311-7 du code de la défense.

personnes et les informations ou supports classifiés et d'en contrôler l'application[47]. L'entreprise doit également élaborer un plan particulier de protection pour chaque PIV identifié[48]. Pour élaborer ces plans, l'opérateur doit s'appuyer sur le guide d'élaboration et les plans-types qui lui sont transmis ; il est d'ailleurs invité à « *se conformer au plan type défini par arrêté du Premier ministre* »[49], tandis que le plan doit être approuvé par les autorités préfectorales[50]. Enfin, un contrôle administratif sera exercé sur l'activité de ces opérateurs d'importance vitale sur lesquels pèseront diverses obligations[51]. Toutes ces obligations mises à la charge de l'entreprise le sont au nom de la sécurité nationale et lui sont financièrement imputées[52].

Si la préservation de la sécurité nationale constitue un impératif au nom duquel des charges sont mises sur les entreprises afin de diminuer la vulnérabilité des entreprises, elle constitue également un enjeu au nom duquel les pouvoirs publics vont s'efforcer d'accompagner la réactivité de ces mêmes entreprises.

2. Accompagner la réactivité des entreprises, un impératif de sécurité nationale

Au-delà de l'impératif pour la sécurité nationale que représente la diminution de la vulnérabilité des entreprises, se profile la question de la réactivité des entreprises en cas de crise. Lorsque la crise est survenue, il apparaît d'importance vitale pour la sécurité nationale que les entreprises puissent réagir et retrouver le plus vite possible l'activité qui est ordinairement la leur. Au-delà et plus largement, c'est en intégrant une véritable culture de la sécurité, y compris, dans les éléments paraissant les plus anodins, que l'entreprise participe de la sécurité nationale.

---

[47] Ce délégué « *représente l'opérateur auprès de l'autorité administrative pour toutes les questions relatives à la sécurité des installations et aux plans de sécurité* », Instruction générale interministérielle n° 6600 du 26 sept. 2008 relative à la sécurité des activités d'importance vitale, p. 24. Plus largement, il participe à l'instruction et à la sensibilisation du personnel en matière de protection du secret. Il est également chargé de la gestion des habilitations et en liaison avec les services enquêteurs, du contrôle des accès aux zones protégées de l'entreprise.

[48] Art. R. 1332-23 du code de la défense. Par ailleurs, si l'entreprise exploite plusieurs PIV, elle doit alors élaborer un document plus global, le plan de sécurité d'opérateur ; art. R. 1332-19 du code de la défense.

[49] Instruction gén. n° 6600 préc., p. 26.

[50] Art. R. 1332-25 du code de la défense. Il convient de préciser qu'afin d'assurer une protection complète du PIV, le plan particulier de protection établi par l'entreprise et sous le contrôle de l'Etat, se voit complété par un plan de prévention externe, dont l'élaboration et la mise en œuvre seront cette fois à la charge de l'Etat ; art. R. 1332-32 du code de la défense.

[51] Obligation de rendre des comptes, d'informer l'administration de toute modification en rapport avec la production, de réaliser des travaux sur ordre de l'administration…

[52] En vertu de l'art. L. 1332-1 du code de la défense, « *les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, sont tenues de coopérer à leurs frais (…) à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste* ».

2.1. La nécessité de la résilience

Le Livre Blanc sur la Défense rendu en 2008, outre qu'il consacra la notion de « sécurité nationale », vint également reconnaître la résilience comme un principe cardinal devant gouverner l'action des pouvoirs publics. La résilience y était définie comme « *la volonté et la capacité d'un pays, de la société et des pouvoirs publics à résister aux conséquences d'une agression ou d'une catastrophe majeures, puis à rétablir rapidement leur capacité de fonctionner normalement, ou à tout le moins dans un mode socialement acceptable. Elle concerne non seulement les pouvoirs publics, mais encore les acteurs économiques et la société civile tout entière* »[53]. Cette résilience s'entend tout à la fois comme une nécessité pour la sécurité nationale, que pour l'entreprise elle-même, au regard de ses intérêts strictement patrimoniaux.

La résilience est un impératif au regard de la sécurité nationale ; « *inséparable de la préservation des entreprises en charge d'activités d'importance vitale, un impératif de résilience s'impose quant à lui à celle en charge de certains réseaux dont le maintien pourrait lui aussi être qualifié "d'importance vitale"* »[54]. Cela explique donc que la loi impose aux opérateurs de certaines activités regardées comme essentielles certaines obligations en matière de continuation de leur activité. C'est ainsi que depuis 2004, la loi exige des exploitants des principaux services publics de première nécessité de prévoir les mesures nécessaires au maintien de la satisfaction des besoins vitaux des populations en toute circonstance et spécialement en cas de crise[55]. Ces réseaux étant de plus en plus fréquemment gérés par des entreprises dénuées de tout lien organique avec l'Etat, En vertu de cette disposition rappelant l'obligation de continuité du service public, « *le cahier des charges type de concession prévoit ainsi que les exploitants des grands réseaux de service public et les opérateurs de communication électronique doivent fixer à l'avance les mesures nécessaires au maintien de la satisfaction des besoins prioritaires de la population en cas de crise* »[56]. La société étant dépendante dans son fonctionnement le plus immédiat et le plus quotidien de l'activité de ces entreprises, il importe que celles-ci soient en mesure d'assurer leur activité ordinaire, tout spécialement en situation de crise. Ces entreprises doivent élaborer un plan interne de crise leur permettant d'anticiper « *les conséquences de la destruction ou du dysfonctionnement de*

[53] *Défense et sécurité nationale - Le livre blanc*, Odile Jacob, 2008, p. 64.
[54] J. Vallotton, « Les entreprises et la sécurité civile », *op. cit.*
[55] Art. L. 732-1 CSI : « *Les exploitants d'un service, destiné au public, d'assainissement, de production ou de distribution d'eau pour la consommation humaine, d'électricité ou de gaz, ainsi que les opérateurs des réseaux de communications électroniques ouverts au public prévoient les mesures nécessaires au maintien de la satisfaction des besoins prioritaires de la population lors des situations de crise* ».
[56] Bertrand Pauvert, obs. sous art. L. 732-1, in *Code de la sécurité intérieure commenté*, Gohin O. & Latour X. dir., Litec, 2014.

leurs installations et élaborer des stratégies de rétablissement du fonctionnement minimal des installations dans un environnement dégradé »[57]. Il est encore imposé que les modalités de retour progressif à un fonctionnement normal du réseau dans les délais les plus raisonnables soient prévues[58]. Afin de faciliter le retour à la normale et les rapports avec les services de secours, les entreprises visées doivent désigner parmi leur personnel, un employé qui devra être l'interlocuteur privilégié des services de l'Etat en cas de crise[59].

D'autres obligations sont également imposées par le code de la sécurité intérieure aux entreprises exploitant des « *ouvrages routiers, ferroviaires ou fluviaux* »[60] et visent à garantir aux services de secours une intervention optimale dans leurs établissements au maintien de leurs capacités opérationnelles dans un environnement dégradé. Préalablement à toute crise, ces entreprises doivent désigner, parmi leur personnel, un agent qui sera l'interlocuteur privilégié des services de secours en cas de crise, afin de faciliter le retour à un fonctionnement normal[61].

Toute crise, qu'elle soit d'origine anthropique ou naturelle, a naturellement pour effet de désorganiser le fonctionnement de l'entreprise, occasionnant d'importants coûts pour toute entreprise, que ce coût soit direct et lié aux réparations à effecteur ou indirect, attaché aux marchés perdus et à la baisse d'activité. Il pourra dès lors être particulièrement nécessaire et intéressant pour l'entreprise de mettre en place un plan lui permettant d'assurer la continuation de ses activités. La continuité d'activité désigne la « *capacité de l'organisation à poursuivre la fourniture de produits ou la prestation de services à des niveaux acceptables et préalablement définis après un incident perturbateur* »[62] et il est de l'intérêt de toute entreprise de pouvoir maintenir la continuité de son activité. Affronter victorieusement une crise suppose une culture du risque et l'acquisition des gestes et méthodes permettant de faire face à l'événement lorsque celui-ci survient et la réalisation par une entreprise d'un plan de continuation d'activité et « *les retours d'expérience des grandes crises récentes montrent que les organisations ayant entrepris une démarche préalable visant à garantir la continuité de*

[57] J. Vallotton, « Les entreprises et la sécurité civile », *op. cit*.
[58] Art. 3. du décret n° 2007-1400 du 28 sept. 2007 relatif à la définition des besoins prioritaires de la population et aux mesures à prendre par les exploitants d'un service destiné au public lors de situations de crise (JO du 30, p. 16134).
[59] Art. L. 732-2 CSI.
[60] Art. L. 732-3 CSI. Le texte vise également les entreprises exploitant les établissements recevant du public les plus importants ; il impose de garantir aux secours la disposition d'une capacité suffisante de communication radioélectrique à l'intérieur de leurs ouvrages et établissements au cours de leur intervention.
[61] Art. L. 732-4 CSI.
[62] Norme ISO 22301, *Sécurité sociétale - Systèmes de management de la continuité d'activité - Exigences*, juin 2012, 3 ; Termes et définitions.

leur activité sont les plus résilientes face aux événements déstabilisants »[63]. L'intérêt bien compris des entreprises sert alors l'impératif de résilience et le nulle surprise à ce que le SGDSN favorise une telle démarche en incitant les entreprises à y recourir.

2.2. La sécurité par le partenariat

Les enjeux liés à la protection de la sécurité nationale ont conduit l'Etat à réaffirmer sa relation aux entreprises ; loin d'être de simples prescripteurs d'obligations pesant sur les entreprises, les pouvoirs publics se veulent partenaires des entreprises. Cette approche partenariale constitue le *credo* nouveau de la défense économique et conduit l'Etat à favoriser la prise de conscience auprès des entreprises des enjeux de sécurité nationale. Cette démarche nouvelle recouvre tant la promotion de l'intelligence économique, que la réflexion sur le secret des affaires ou la sécurité des systèmes d'information.

Depuis 2002, le contenu de la notion de « défense économique » a été redéfini et se décompose entre la défense économique dite régalienne et la partenariale. Cette dernière désigne les modalités d'action d'un Etat qui se veut stratège et partenaire des entreprises ; elle peut se décomposer en « *politique de sécurité que les entreprises et la collectivité doivent s'imposer à elles-mêmes, comme la protection et la sécurité des systèmes d'information et les mesures découlant d'éventuelles dépendances stratégiques ; politique de protection du patrimoine (…) ; politique d'ouverture à la concurrence et à la mondialisation, s'appuyant notamment sur le développement de la maîtrise du savoir au moyen de l'intelligence économique, volet de la défense économique en relation avec l'information économique ouverte* »[64]. Dans cette perspective qui tend à être désormais privilégiée[65], les pouvoirs publics s'efforcent de sensibiliser les acteurs économiques aux enjeux de sécurité nationale et promeuvent notamment auprès des entreprises des stratégies de protection de leur patrimoine[66] ou de leur systèmes d'information. L'Etat va alors soutenir l'activité de ses entreprises en leur fournissant un soutien logistique en la matière et en les incitant à renforcer leur sécurité interne afin de conquérir ou conserver au mieux leur place sur les marchés. L'idée étant que la préservation des intérêts des entreprises est un moyen de préserver ceux de la nation.

[63] SGDSN, *Guide pour réaliser un plan de continuité d'activité*, 2013, p. 3
[64] Circ. du 14 fév. 2002 relative à la défense économique (JO du 23 mars, p. 5164).
[65] La défense économique régalienne s'attache, pour sa part, au fonctionnement général de l'économie ; elle vise à prévenir les dysfonctionnements économiques et préparer les crises susceptibles d'intervenir, par l'établissement de programmes de prévention, d'action ou de réaction à celles-ci.
[66] Qu'il s'agisse de patrimoine physique ou immatériel.

C'est en particulier par la promotion de ce qu'il est désormais convenu d'appeler l'intelligence économique que se déploie cette action de l'Etat aujourd'hui. L'intelligence économique peut être définie comme « *l'ensemble des actions coordonnées de recherche, de traitement et de distribution en vue de son exploitation, de l'information utile aux acteurs économiques* »[67]. La charge de fixer les orientations générales de la politique de protection et d'intelligence économique relève du ministre chargé de l'économie. L'intelligence économique recouvrira l'ensemble des mesures devant être menées dans l'intérêt des entreprises et des acteurs économiques ; cette politique est menée par un délégué interministériel à l'intelligence économique placé auprès du Premier ministre[68]. Le délégué possède pour mission d'élaborer et proposer la politique publique d'intelligence économique ; il lui appartient notamment de collecter toutes les informations utiles, auprès des agences gouvernementales ayant pour fonction de recueillir ces informations et de les diffuser auprès des opérateurs économiques nationaux, au moyen d'un réseau de correspondants dans les services déconcentrés de l'Etat ainsi que dans les ambassades et consulats.

Dans le cadre de la défense économique partenariale, un champ particulier mérite encore l'attention c'est celui de la sécurité des systèmes d'information. Il s'agira en particulier pour l'Etat d'inciter les entreprises à adopter des comportements d'autoprotection de leurs données. Nos sociétés sont aujourd'hui totalement dépendantes des moyens d'information et de communication, lesquels fonctionnent dans un tissu informatique global qualifié de cyberespace ; celui-ci, contrairement à l'espace physique, est sans frontière, évolutif et anonyme, constituant un espace dans lequel l'identification d'un agresseur ou d'une menace est délicate. Au-delà de la seule nécessité de se protéger d'attaques visant directement l'outil de défense, il convient encore de se prémunir d'attaques informatiques qui conduiraient à mettre en cause des informations sensibles d'un point de vue économique. Or, la France a eu une prise de conscience tardive des enjeux liés à la sécurité des systèmes d'information[69],

---

[67] Henri Martre, *Intelligence économique et stratégie des entreprises*, La Doc. fr., 1994, p. 11.

[68] Décret n° 2013-759 du 22 août 2013 relatif au délégué interministériel à l'intelligence économique (JO du 23) ; ce délégué est la dernière mouture d'une organisation remontant au milieu des années 1990. Le 1er avril 1995 fut institué un comité pour la compétitivité et la sécurité économique (décret n° 95-350, JO du 4, p. 5375) ; comité remplacé en 2003 par un haut responsable chargé de l'intelligence économique (décret n° 2003-1230 du 22 déc. 2003 ; JO du 24, p. 22.056) alors placé auprès du secrétaire général de la défense nationale. En 2009 ses services sont réorganisés et placés sous la dépendance du ministère de l'économie (décret n° 2009-1122 du 17 sept. 2009 relatif au délégué interministériel à l'intelligence économique ; JO du 18, p. 15.229).

[69] « *Si les risques soulevés par la cybercriminalité sur l'économie avaient déjà été identifiés depuis longtemps, l'optique d'un risque pesant plus particulièrement sur la sécurité des Etats est plus récente* » relevait Jean-Marie Bockel, *La cyberdéfense : un enjeu mondial, une priorité nationale*, rapport d'information n° 681, Sénat, 18 juil. 2012, p. 11. C'est en effet dès 2006 qu'un rapport au Premier ministre constatait : « *la France accuse un retard préoccupant face aux impératifs de sécurité des systèmes d'information, tant au niveau de l'Etat qu'au niveau*

occasionnant un renouveau de la réflexion sur la cybersécurité. Dans le fil du rapport Romani[70], c'est le Livre Blanc de 2008 qui s'intéressera à la question de la sécurité des systèmes d'information et aux attaques informatiques[71]. Elevée au rang de d'enjeu de sécurité nationale, la cybersécurité a conduit à la création de l'Agence Nationale de la Sécurité des Systèmes Informatiques (ANSSI). L'ANSSI, créée en 2009[72], assure une mission classique de défense des systèmes d'information de l'Etat, mais possède également pour mission de jouer un rôle de conseil aux opérateurs d'importance vitale[73], signe que la sécurité informatique des entreprises constitué bien un enjeu pour l'a sécurité nationale et l'Etat.

Au terme de cet examen des liens entre l'entreprise et la sécurité nationale se dessine un paysage contrasté. De fait, à la récente prise de conscience des enjeux pour la sécurité nationale d'un tissu d'entreprise compétitives ne peut manquer de répondre le constat des lacunes d'un Etat sur la défensive et dont la légitimité même à intervenir dans le champ économique est contestée. Si la mise en avant d'une démarche partenariale vise à combler les lacunes des modalités d'intervention de l'Etat contemporain, il reste néanmoins un point cardinal à envisager et que l'on ne pourra négliger à l'avenir, celui du financement des entreprises des secteurs économiques porteurs d'intérêts nationaux stratégiques[74].

---

des entreprises, quelques grands groupes mis à part », Pierre Labordes, *La sécurité des systèmes d'information : un enjeu majeur pour la France*, La Doc. fr., 2006, p. 90

[70] Roger Romani, *Cyberdéfense : un nouvel enjeu de sécurité nationale*, rapport d'information n° 449, Sénat, 8 juil. 2008.

[71] *Défense et Sécurité nationale - Le Livre Blanc*, Odile Jacob & La Doc. fr., 2 t., 2008. Après le constat des carences de la France, le Livre Blanc appelait à la création d'une agence chargée de la sécurité des systèmes d'information et devant *« mettre en œuvre une capacité centralisée de détection et de défense face aux attaques informatiques. Elle sera dotée des moyens de faire développer et d'acquérir les produits de sécurité essentiels à la protection des réseaux les plus sensibles de l'Etat. Elle sera également chargée d'assurer une mission de conseil du secteur privé, notamment dans les secteurs d'activité d'importance vitale* », *Livre Blanc*, p. 182.

[72] Décret n° 2009-834 du 7 juil. 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information » (JO du 8).

[73] L'ANSSI constitue également un réservoir de compétences destiné à apporter son expertise et son assistance technique, outre aux administrations, aux opérateurs d'importance vitale.

[74] Signe de cette prise de conscience, le délégué interministériel à l'intelligence économique est chargé de proposer « *des mesures visant à faciliter le financement des entreprises des secteurs économiques porteurs d'intérêts nationaux stratégiques* », décret n° 2013-759 préc.